PATENT
Docket No. **VIV/0003.01**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Gregor P. Freund et al.	Examiner: Divecha, Kamal B
Serial No.: 09/944,057	Art Unit: 2151
Filed: August 30, 2001	APPEAL BRIEF
For: System Providing Internet Access Management with Router-based Policy Enforcement	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

BRIEF ON BEHALF OF GREGOR P. FREUND ET AL.

This is an appeal from the Final Rejection mailed 05/05/2008, in which currently-pending claims 1-64 stand finally rejected. Appellant filed a Notice of Appeal on 08/07/2008. This brief is submitted electronically in support of Appellant's appeal.

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest is assignee Check Point Software Technologies, Inc. located at 800 Bridge Parkway, Redwood City, CA 94065.

2. RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to Appellant, the Appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS

The status of all claims in the proceeding is as follows:

Rejected: Claims 1-64

Allowed or Confirmed: None

Withdrawn: None

Objected to: None

Canceled: None

Identification of claims that are being appealed: Claims 1-64

An appendix setting forth the claims involved in the appeal is included as the last section of this brief.

4. STATUS OF AMENDMENTS

Three Amendments have been filed in this case. Appellant filed an Amendment on 03/02/2005 in response to a non-final Office Action dated 12/02/2004, and filed an Amendment After Final on 06/08/2005 in response to a Final Rejection dated 04/07/2005. Additionally, Appellant filed an Amendment on 02/29/2008 in response to a non-final Office Action dated 10/31/2007 (which withdrew the Final Rejection and reopened prosecution). In the Amendments, the pending claims have been amended in a manner which Appellant believes clearly distinguished the claimed invention over the art of record, for overcoming the art rejections. In response to the Examiner's Final Rejection dated 05/05/2008, Appellant filed a Notice of Appeal. Appellant has chosen to forgo filing an Amendment After Final which might further limit Appellant's claims, as it is believed that further amendments to the claims are not warranted in view of the art.

Accordingly, no Amendments have been entered in this case after the date of the Final Rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Appellant asserts that the art rejections herein fail to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 1**: in a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (see, e.g., Appellant's specification at page 19, lines 22-27; see also Fig. 3 at 310, 320, 330, 340, 350, and specification at page 20, lines 12-22), a method for managing Internet access based on a specified access policy, the method comprises steps of: transmitting a plurality of challenges over a period of time from the client premises equipment to each client computer, for determining whether a given client computer remains in compliance with the specified access policy during the period of time (see, e.g., Appellant's specification at page 20, lines 23-31; see also router compliance table (Fig. 3 at 312) analysis, described at page 21, lines 10-18; and see also router compliance table processing steps in Fig. 9 at 920, 930, 940 and accompanying specification description at page 38, lines 7-13); transmitting a response from at least one client computer back to the client premises equipment for responding to each of the challenges that has been issued (see, e.g., Appellant's specification at page 20, lines 28-31; see also lines of communication, illustrated in Fig. 3, between router 310 and computers 320, 330, 340; and see also page 21 at lines 10-12, which describe the receipt and storage of client responses); and blocking Internet access for any client computer that does not respond appropriately to any challenge issued to it (see, e.g., Appellant's specification at page 21, lines 12-30; see also Fig. 3 showing redirection of (noncompliant) computer 330 to sandbox server 360; and see also Fig. 9, generally at 920-980, and especially step 970).

Appellant further asserts that the art rejections herein fail to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 24**: in a system comprising one or more client computers connected to the Internet by client premises equipment

serving a routing function for client computers (see, e.g., Appellant's specification at page 19, lines 22-27; see also Fig. 3 at 310, 320, 330, 340, 350, and specification at page 20, lines 12-22), a method for managing Internet access based on a specified access policy, the method comprises steps of: transmitting a plurality of challenges over a period of time from the client premises equipment to each client computer, for determining whether a given client computer is in compliance with the specified access policy during the period of time (see, e.g., Appellant's specification at page 20, lines 23-31; see also router compliance table (Fig. 3 at 312) analysis, described at page 21, lines 10-18; and see also router compliance table processing steps in Fig. 9 at 920, 930, 940 and accompanying specification description at page 38, lines 7-13); transmitting a response from at least one client computer back to the client premises equipment for responding to the challenge that has been issued (see, e.g., Appellant's specification at page 20, lines 28-31; see also lines of communication, illustrated in Fig. 3, between router 310 and computers 320, 330, 340; and see also page 21 at lines 10-12, which describe the receipt and storage of client responses); and redirecting a request for Internet access by any client computer that does not respond appropriately to any challenge issued to it to a sandbox server (see, e.g., Appellant's specification at page 19, line 24 to page 20, line 4; Appellant's specification at page 21, lines 12-30; see also Fig. 3 showing redirection of (noncompliant) computer 330 to sandbox server 360 and accompanying description at p. 21, lines 26-30; and see also Fig. 9, generally at 920-980, and especially step 970).

Appellant also asserts that the art rejections herein fail to teach or suggest all of the claim limitations of Appellant's claimed invention, where the claimed invention comprises the embodiment set forth in **independent claim 45**: a system for regulating Internet access by client computers comprising (see, e.g., Appellant's specification at page 20, lines 23-31; see also router compliance table (Fig. 3 at 312) analysis, described at page 21, lines 10-18; and see also router compliance table processing steps in Fig. 9 at 920, 930, 940 and accompanying specification description at page 38, lines 7-13): an access policy governing Internet access by the client computers (see, e.g., Appellant's specification at page 21, lines 19-30; at page 22, line 28 to page 23, line 4; see also page 28, line 6 to page 30, line 22; and Fig. 5 at 500 and Fig. 6 at 600); client premises equipment serving a routing function for each client computer to be regulated and

capable of issuing a plurality of challenges over a period of time to each client computer, for determining whether a given client computer is in compliance with the access policy during the period of time (see, e.g., Appellant's specification at page 20, lines 23-31; see also router compliance table (Fig. 3 at 312); one or more client computers which can connect to the Internet and at least one of which can respond to challenges issued by the client premises equipment (see, e.g., Appellant's specification at page 20, lines 28-31; see also lines of communication, illustrated in Fig. 3, between router 310 and computers 320, 330, 340; and see also page 21 at lines 10-12, which describe the receipt and storage of client responses); and an enforcement module for selectively blocking Internet access to the Internet for any client computers that fail to respond in a manner that would establish that they are in compliance with the access policy (see, e.g., Appellant's specification at page 21, lines 12-30; see also Fig. 3 showing redirection of (noncompliant) computer 330 to sandbox server 360; and see also Fig. 9, generally at 920-980, and especially process step 970).

Appellant additionally argues based on **dependent claims 6 and 30** which include a claim limitation pertaining to: wherein said initial message comprises a "client hello" packet (see, e.g., Appellant's specification at page 24, lines 1-9; see also transmission of a "client hello" packet by computer 320 to router 310 as illustrated in Fig. 3).

Appellant additionally argues based on **dependent claims 13-16, 34, 42-44, 56 and 58-60** which include claim limitations pertaining to: wherein said access policy specifies applications that are allowed Internet access, and wherein said applications are specified by executable name and version number that are acceptable (see, e.g., Appellant's specification at page 28, line 30 to page 29, line 13; and program settings panel 530 shown on the bottom half of Fig. 5).

Appellant additionally argues based on **dependent claims 23, 25, 26, 40, 41 and 62-64** which include claim limitations pertaining to a "sandbox" limitation (see, e.g., Appellant's specification at page 19, line 19 to page 20, line 4; additionally, see the right side of Fig. 3 which shows a sandbox server 360, which is a computer server that is located somewhere on the Internet).

6. GROUNDS OF REJECTION TO BE REVIEWED

The grounds presented on appeal are:

(1st) Whether claims 1-5, 7-12, 17-22, 24, 27-29, 31-33, 35-39, 45-55, 57 and 61 are unpatentable under 35 U.S.C. 103(a) as being obvious over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Phillips et al. (hereinafter Phillips, US 6,721,555 Bl);

(2nd) Whether claims 6 and 30 are unpatentable under 35 U.S.C. 103(a) as being obvious over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Phillips et al. (hereinafter Phillips, US 6,721,555 Bl), and further in view of Kadyk et al. (hereinafter Kadyk, US 6,996,841 B2);

(3rd) Whether claims 13-16, 34, 42-44, 56 and 58-60 are unpatentable under 35 U.S.c. 103(a) as being obvious over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Phillips et al. (hereinafter Phillips, US 6,721,555 Bl), and further in view of "Official Notice";

(4th) Whether claims 23, 25, 26, 40, 41 and 62-64 are unpatentable under 35 U.S.C. 103(a) as being obvious over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Phillips et al. (hereinafter Phillips, US 6,721,555 B1), and further in view of Shrader et al. (hereinafter Shrader, US 6,026,440); and

(5th) Whether claims 7, 41 and 52 are indefinite under 35 U.S.C. 112, second paragraph, for failing to particularly point out and distinctly claim the subject matter which Appellant regards as the invention.

7. ARGUMENT

A. First Ground: Claims 1-5, 7-12, 17-22, 24, 27-29, 31-33, 35-39, 45-55, 57 and 61 rejected under Section 103

1. General

Under Section 103(a), a patent may not be obtained if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. To establish a prima facie

case of obviousness under this section, the Examiner must establish: (1) that there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings, (2) that there is a reasonable expectation of success, and (3) that the prior art reference (or references when combined) must teach or suggest all the claim limitations. (See e.g., MPEP 2142). The references cited by the Examiner fail to meet these conditions.

2. Claims 1-5, 7-12, 17-22, 24, 27-29, 31-33, 35-39, 45-55, 57 and 61

Claims 1-5, 7-12, 17-22, 24, 27-29, 31-33, 35-39, 45-55, 57 and 61 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Phillips et al. (hereinafter Phillips, US 6,721,555 Bl). The Examiner's rejection of claim 1 is representative:

> As per claim 1, Stockwell discloses a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (fig. 1: the computers connected to internal network, col. 4 L21-42: a firewall gateway), a method for managing Internet access based on a specified access policy (col. 1 L5- 10, col. 3 LI6-54, col. 5 LI6-22: access policies), the method comprising:
> a challenge/response sequence for determining whether a given client computer is in compliance with said specified access policy (col. 5 L16 to col. 6 L67, col. 9 LI-60); blocking Internet access for any client computer that does not respond appropriately to any challenge issued to it (col. 5 L16 to col. 6 L67, col. 9 LI-60: blocking the Internet access by dropping the connection, col. 11 L5-67).
> However, Stockwell does not explicitly disclose the process of transmitting plurality of challenges over a period of time from said client premises equipment to each client computer for determining whether a given client computer remains in compliance with policy during period of time and transmitting a response from at least one client computer back to said client premises equipment for responding to each of challenges that has been issued.
> Phillips explicitly discloses an Internet access device that performs the process of transmitting a plurality of challenges over a period of time from said client premises equipment to each client computer for determining whether the given client computer remains in compliance and transmitting a response from at least one client computer back to said client premises equipment for responding to each of said challenges that has been issued (col. 4 L50- 67, col. 5 L6 to col. 6 L28, col. 7 L4-9: IFW with router).
> Therefore, it would have been obvious to a person of ordinary skilled in the art at

the time the invention was made to modify Stockwell in view of Phillips in order transmit a plurality of challenges over period of time to the client computer and receiving a response to the challenges.

The Examiner acknowledges that Stockwell does not explicitly disclose the process of "transmitting a plurality of challenges over a period of time from said client premises equipment to each client computer, for determining whether a given client computer remains in compliance with said specified access policy during said period of time." However, the Examiner contends that this missing feature is provided by Phillips.

Stockwell describes a system and method for regulating the flow of internetwork connections through a firewall having a network protocol stack which includes an Internet Protocol (IP) layer. Based on the parameters characteristic of a connection request, the Stockwell system determines if authentication is required (by a corresponding rule). If authentication is required by the rule, an authentication protocol is activated and the connection is activated if the authentication protocol is completed successfully. Phillips, on the other hand, describes a system for facilitating device authentication in a wireless communications system. For the portions cited by the Examiner (i.e., columns 4-7), Phillips describes the CHAP (Challenge Handshake Authentication Protocol) which is designed for inclusion in PPP (point-to-point protocol) stacks. As is well understood in the prior art, authentication protocols are often (if not universally) employed to verify that users attempting to access a particular service are authorized users. In the case of the Phillips teaching, Phillips points to the example that an IWF (an "Interworking Function," which includes one or more routers and modem pools for routing calls between the wireless infrastructure and the Internet) may wish to verify that the user of a TE2 device (Terminal Equipment) is an authorized user of Internet access service offered via the IWF. As will be shown below, the combined references fail to teach each and every element set forth in the rejected claims and therefore fail to establish obviousness of the claimed invention under Section 103.

At its core architectural level, Appellant's invention is fundamentally different from the combination of Stockwell with Phillips. By way of brief review, Appellant's invention includes a router-side client management protocol (CMP) installed and operational on the client's (i.e., the user's) router (client premises equipment). This

operates in conjunction with a client-side security module of the present invention that is installed and running on the user's computers. This security module continually enforces **compliance** with an access or security policy (i.e., rules set up by an organization, for establishing permitted access activities of a user's computer). In Appellant's system, for example, a given security policy may specify which particular applications are allowed Internet access, thereby allowing users (including administrators) to block spyware and other malware from accessing the Internet from a given client machine, thereby preventing the transmission of confidential or sensitive information from the client computer (e.g., desktop computer, laptop, or the like) to third party perpetrators on the Internet). Appellant's claimed invention, which issues periodic challenges to client computers (i.e., user's computers), requires that a given client computer remain in **compliance** with the specified access policy (during a relevant period of time). **Importantly, the concern addressed by Appellant's invention is a computer's continued compliance with applicable security policies (e.g., that it complies with a corporate security policy's requirement that a user's machine have up-to-date antivirus software), not its authentication or identity (e.g., username and password).** The Examiner attempts to buttress the deficiencies of Stockwell by contending that Phillips supplies the missing teaching of compliance enforcement -- however such a contention by the Examiner is a gross overstatement of the teaching of Phillips. These differences between Appellant's compliance enforcement mechanism and Phillip's authentication mechanism will now be examined in further detail.

Authentication protocols (including handshakes/challenges and exchange of hashed passwords or shared secrets) are well known in the prior art, and Appellant certainly makes no claim to have invented those concepts. Phillips, if the title of his patent is to believed, describes "System and method for facilitating device authentication in a wireless communications system." The problem addressed by Appellant's invention, however, does not pertain at all to authentication. In fact, Appellant's invention does not even provide authentication services (as those are already assumed to be adequately provided by existing infrastructure, such as network operating system (OS)). Instead, the particular issue addressed by Appellant's invention is to make sure that a client-side security module is both installed and properly operating on each local computer. Here,

"properly operating" means that each client computer not only has the client-side security module installed but each computer is continually checked to make sure it is operating pursuant to security policies (applied by the client-side security module). The very specific issue is one of ensuring continued compliance with applicable security policies (that a given organization requires in order to use its network). This is **not** the issue of identifying or authenticating the user's computer (which has already been carried out by the network OS), which is what Phillips pertains to (in the context of Terminal Equipment operating in a wireless environment). Succinctly stated Appellant's invention, in contrast to the cited prior art, issues challenges to a client computer **for determining whether the client computer is in compliance with the above-described access policy governing Internet access by client computers**.

Why does continual monitoring of user devices for compliance with an organization's security policy even matter? As more and more computers are now connected to the Internet, either directly (e.g., over a dial-up or broadband connection with an Internet Service Provider or "ISP") or through a gateway between a LAN and the Internet, previously closed computing environments are now open to a worldwide network of computer systems that is the Internet. This has led to (well-publicized) attacks by perpetrators (hackers) capable of damaging local computer systems, misusing those systems, or stealing proprietary data and programs. For example, every user today knows that it is critical to run antivirus software to prevent infiltration by computer viruses, "Trojan horse" programs, and other malware. However, even the best intending user may, on occasion, fail to operate such software properly or have appropriate updates (especially, up-to-date virus definitions) for the software. In an important networking environment (e.g., major corporation or government network), such a failing of a single user (or his/her machine) may provide an entry point for a perpetrator, with catastrophic consequences for the network. In such networks, reliance on "good intentions" of each individual user to maintain his or her computer in accordance with applicable security policies (of the firm) is simply not enough. Instead, what is needed is a solution that requires the user to have his or her computer come into compliance and stay in compliance at all relevant times (namely, while connected) with the applicable security policies of the firm.

Significantly, Appellant's claimed invention includes a novel technique to ensure that each user computer remains in compliance with applicable security policies, otherwise the computer's access is blocked (thus removing the possibility that that computer may serve as a point of vulnerability for the network). For example, the system administrator may establish a policy requiring that a specific version of the security solution or a specific virus protection program is operational on each user's computer. Appellant's claimed methodology operates to evaluate whether or not each local computer is in compliance with the specified policy -- again note that authentication of a given computer is neither an issue nor is it tested at this juncture. In Phillips' environment, which is directed to authentication in a wireless communication system, devices may come and go so rechecking authenticity or identity of devices would certainly seem to make sense (for the problem Phillips is addressing). Appellant's methodology isn't attempting to authenticate (or repeatedly authenticate) the user's computer with handshake or username/password challenges, however, as such authentication is already addressed by other subsystems (e.g., the network OS). Importantly, verifying authentication (a la Phillips) confirms the identify of the device but tells nothing about whether that device has been set up to adhere to a firm's security policies and tells nothing about whether that device in fact remains compliant with those policies from one moment to the next.

Instead of repeatedly testing authentication in the manner of Phillips, Appellant's methodology of checking ongoing compliance with specified security requirements is a far more complex task. By way of brief review, Appellant's solution internally operates as follows. (The following is provided for background and context to assist the reader with understanding the technology underlying the present invention, and there is no intention to suggest that "Appellant is arguing" each and every feature is in present in the claims, as such would impractical, unwise, and not necessitated by the art of record.) Every few seconds Appellant's router-side client management protocol (CMP) component sends out a communication via Internet broadcast to connected computers that is described as a "router challenge." This router challenge -- which is repeatedly initiated by the router and not by the user or his/her computers -- requires a response from the (connected) computers within a few seconds. Computers that have the client-side

security module installed **and** are compliant (e.g., comply with any policy required for the client device) may return an appropriate response to the router challenge. Any computer that does not have the client-side security module installed or is otherwise noncompliant (i.e., fails to comply with a policy requirement) is unable to respond to the router challenge in an appropriate manner, and thus will be blocked from Internet access by the client premises equipment (router). As should be evident at this point, **Appellant's approach has the particular advantage that a given client computer must at all times be able to establish -- and continue to re-establish -- its compliance with required security policies.** The moment a client computer falls out of compliance (e.g., due to a user lapse, such as the computer's virus definition file falling out-of-date), it is blocked from access. The Examiner contends that Phillips teaches Appellant's claim limitation pertaining to determining whether a given client computer remains in compliance with a specified access policy over a given period of time, yet the Phillips patent itself mentions nothing of the sort. The Phillips patent does not even mention the words "compliance" or "policy." Given that Phillips limits itself to testing authentication and is wholly unconcerned about any compliance monitoring, Phillips at best teaches away from Appellant's claimed approach.

Appellant's invention does not permit or block requests for access based on user login or other authentication information. Instead, **Appellant's system determines whether a given client computer is in compliance with the specified access policy** governing Internet access. If the client computer is not in compliance with the access policy, Appellant's invention blocks access to the Internet. These features are specifically described in Appellant's claims, including, for example, in Appellant's claim 1 which includes the following claim limitations:

> 1. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:
> transmitting a plurality of challenges over a period of time from said client premises equipment to each client computer, **for determining whether a given client computer remains in compliance with said specified access policy during said period of time**;
> transmitting a response from at least one client computer back to said client

premises equipment for responding to each of said challenges that has been issued; and
blocking Internet access for any client computer that does not respond appropriately to any challenge issued to it.

(Emphasis added.)

It is Appellant's argument and position that the foregoing specific claim limitations in independent claim 1 (as well as independent claims 24 and 45) are not reproducible from teachings or suggestions of Stockwell combined with Phillips. As shown above, Appellant's invention provides for client premises equipment to regulate access to the Internet by client computers. The decision about whether to allow Internet access by a given computer is based on compliance by the given computer with the above-described security or access policy. This is different from authentication approaches which are testing a user's device for access based on login information (e.g., user name and password) supplied by the user.

3. Conclusion

All told, Appellant's claimed invention provides around-the-clock protection of networks so that the moment that any client computer lapses into noncompliance (e.g., fails to comply with applicable corporate security policies), that computer can be effectively kicked off (i.e., denied access). Such a result is not possible with the combination of Stockwell and Phillips, as those combined references provide no teaching or suggestions for continual, router-initiated monitoring of client computers. In Appellant's approach, client computers must repeatedly and unconditionally "prove up" their compliance. In Appellant's invention, the router is constantly issuing challenges to the client computer for determining whether the client computer is in compliance with the applicable access policy governing Internet access by client computers. It is not possible to coax such a teaching from the combination of Stockwell and Phillips. As these references do not teach or suggest all of the claim limitations of Appellant's independent claims of this group of rejecting claims (and other dependent claims thereof), it is respectfully submitted that the claims distinguish over these combined references and that

the Examiner's rejection under Section 103 should not be sustained.

B. Second Ground: Claims 6 and 30 rejected under Section 103

1. Claims 6 and 30

Claims 6 and 30 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Phillips et al. (hereinafter Phillips, US 6,721,555 Bl), and further in view of Kadyk et al. (hereinafter Kadyk, US 6,996,841 B2). Here, the Examiner repeats the rejection based on Stockwell and Phillips above, but adds Kadyk for transmission of the "client hello" limitation. The claims are believed to be allowable for at least the reasons stated above pertaining to the rejection of the base claims (i.e., the parents of claims 6 and 30) on the basis of Stockwell and Phillips.

Moreover, the claims are believed to be allowable for the following additional reasons. Phillips describes user identity information (e.g., username and password) for authenticating a user. After the user's identity is authenticated, Phillips' system (like the previously-cited Fuh and Elliot systems, in prior Office Actions) permits (at best, based on the Examiner's combination with Stockwell) particular types of network traffic initiated by that particular user. This is not Appellant's claimed approach. Appellant's approach provides for making the decision about whether or not to permit access based on a client computer's then-current compliance with any applicable access policy. The "client hello" limitation of the rejected claims of this group make it clear that Appellant's claimed approach is directed to device-to-device (i.e., router-to-computer) compliance verification irrespective of what the user is doing (including, even if the user is in fact authenticated). The combined references do not teach this limitation.

2. Conclusion

For the reasons stated, it is respectfully submitted that Appellant's claims of this group distinguish over the prior art and that this rejection under Section 103 should not be sustained.

C. Third Ground: Claims 13-16, 34, 42-44, 56 and 58-60 rejected under Section 103

1. Claims 13-16, 34, 42-44, 56 and 58-60

Claims 13-16, 34, 42-44, 56 and 58-60 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Phillips et al. (hereinafter Phillips, US 6,721,555 Bl), and further in view of "Official Notice". Here, the Examiner repeats the rejection based on Stockwell and Phillips, but adds Official Notice for Appellant's limitation that compliance (by which access may be granted) may be predicated on a certain application name or version (e.g., that a certain version of antivirus software be installed). The claims are believed to be allowable for at least the reasons stated above pertaining to the rejection of the base claims (i.e., parent claims 1, 24, and 45) on the basis of Stockwell and Phillips.

Moreover, the claims are believed to be allowable for the following additional reasons. As previously described, Phillips describes user identity information (e.g., username and password) for authenticating a user. After the user's identity is authenticated, Phillips' system (like the previously-cited Fuh and Elliot systems) permits (at best, based on the Examiner's combination with Stockwell) particular types of network traffic initiated by that particular user (i.e., based on that user's identity). This is not Appellant's claimed approach. Appellant's claimed approach, as set forth in these rejected claims, provides for determining whether or not to permit Internet access based on compliance with an access policy which specifies particular applications which are approved for Internet access. "Particular applications" in this context may mean that a certain version (namely, the latest up-to-date version) of antivirus software must be installed, for example. The combined references have no facility to predicate access on the basis that certain software be installed on the client computer.

2. Conclusion

For the reasons stated, it is respectfully submitted that Appellant's claims of this group distinguish over the prior art and that this rejection under Section 103 should not be sustained.

D. Fourth Ground: Claims 23, 25, 26, 40, 41 and 62-64 rejected under Section 103

1. Claims 23, 25, 26, 40, 41 and 62-64

Claims 23, 25, 26, 40, 41 and 62-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stockwell et al. (hereinafter Stockwell, US 5,950,195) in view of Phillips et al. (hereinafter Phillips, US 6,721,555 B1), and further in view of Shrader et al. (hereinafter Shrader, US 6,026,440). Here, the Examiner repeats the rejection based on Stockwell and Phillips, but adds Shrader for Appellant's "sandbox" limitation. The claims are believed to be allowable for at least the reasons stated above pertaining to the rejection of the base claims (i.e., parent claims 1, 24, and 45) on the basis of Stockwell and Phillips. Importantly, in these claims, the connection is redirected to a sandbox server based on noncompliance of the client computer itself (which is repeatedly tested), not on the lack of authentication of the user (Phillips) or conditional triggering of a rule based on a certain network traffic occurring (Stockwell).

2. Conclusion

For the reasons stated, it is respectfully submitted that Appellant's claims of this group distinguish over the prior art and that this rejection under Section 103 should not be sustained.

E. Fifth Ground: Claims 7, 41 and 52 rejected under Section 112, second paragraph

1. Claims 7, 41 and 52

Claims 7, 41 and 52 stand rejected as being indefinite under 35 U.S.C. 112, second paragraph, for allegedly failing to particularly point out and distinctly claim the subject matter which Appellant regards as the invention. In particular, the Examiner states that the phrase "others" renders the claims indefinite because it is unclear which one of the plurality of clients the term is referring to, thereby rendering the scope of the claim(s) unascertainable.

At the outset, it is noted that the Examiner complains about the phrase "others" yet that phrase or word does <u>not</u> appear in the claims. In any event, Appellant does use

the phrase "other client computers" and, for the reasons set forth below, it is respectfully submitted that use of "other" in that phrase is not ambiguous. Moreover, it is worth noting that Appellant (and Appellant's attorney) accord near universal deference to examiners in regards to Section 112, second paragraph issues. However in the present rejection, Appellant has carefully reviewed the complained-about word and surrounding claim language, and respectfully submits that the rejection is improper.

Webster's Dictionary defines the word "other" to mean: "being the one or ones distinct from that or those first mentioned or implied." In other words, as Webster's points out, this means "not the same" or "different" and gives an example of "Any *other* color would have been better." (See, e.g., *www.merriam-webster.com/dictionary/other*) Turning to Appellant's specific claim language, objected-to claim 7 for example states:

> 7. The method of claim 1, wherein said client premises equipment is capable of *permitting Internet access by selected client computers* and *denying access to other client computers*.
>
> (Emphasis added.)

Applicant's use of "other" above is in reference to "the one or ones distinct from that or those first mentioned or implied." Specifically, Appellant's reference to "other client computers" is a reference to client computers that are "not the same" or "different" than the first-mentioned or implied -- that is, the "selected client computers."

Moreover for this application, Appellant has filed three prior Amendments and a prior Appeal Brief (as well as two amended Appeal Briefs thereof). Given the protracted prosecution history here and Appellant's repeated good-faith efforts to address multiple iterations of prior art rejections (to the tune of six responses, not including the present response), why all of a sudden is the Examiner now alleging that this original claim language is ambiguous? The Examiner has lodged the rejection at a point in time that is prejudicial to the efficient and cost effective prosecution of the present application as addressing the rejection in the manner required by the Examiner would require still yet another Amendment (and possibly purchase of an RCE). With all due respect to the

Examiner, it is respectfully submitted that the complained-about language is not ambiguous and that the rejection is improper and should not be sustained.

F. Conclusion

The present invention greatly improves the ease and efficiency of the task of managing Internet access, including preventing access by computers that do not conform to a security policy governing types of access permitted, which is currently in force (e.g., by a corporate IT department). It is respectfully submitted that the present invention, as set forth in the pending claims, sets forth a patentable advance over the art.

In view of the above, it is respectfully submitted that the Examiner's rejections under 35 U.S.C. Section 103 should not be sustained. If needed, Appellant's undersigned attorney can be reached at 408 884 1507. For the fee due for this Appeal Brief, please refer to the attached Fee Transmittal Sheet. This Brief is submitted electronically.

Respectfully submitted,

Date: November 7, 2008

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX

8. CLAIMS APPENDIX

1. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:

transmitting a plurality of challenges over a period of time from said client premises equipment to each client computer, for determining whether a given client computer remains in compliance with said specified access policy during said period of time;

transmitting a response from at least one client computer back to said client premises equipment for responding to each of said challenges that has been issued; and

blocking Internet access for any client computer that does not respond appropriately to any challenge issued to it.

2. The method of claim 1, wherein a client computer that does not respond at all is blocked from Internet access.

3. The method of claim 1, wherein a client computer that responds with a particular predefined code indicating non-compliance is blocked from Internet access.

4. The method of claim 1, wherein a client computer that responds with a particular predefined code indicating compliance is permitted Internet access.

5. The method of claim 1, further comprising:

before receipt of a challenge, transmitting an initial message from a particular client computer to the client premises equipment, for requesting the client premises equipment to transmit a challenge to that particular client computer.

6. The method of claim 5, wherein said initial message comprises a "client hello" packet.

7. The method of claim 1, wherein said client premises equipment is capable of permitting Internet access by selected client computers and denying access to other client computers.

8. The method of claim 1, wherein said access policy specifies rules that govern Internet access by the client computers.

9. The method of claim 8, wherein said step of blocking Internet access includes:

determining whether permitting Internet access for a given client computer would violate any of said rules, and

if permitting such Internet access would violate any of said rules, denying Internet access for that client computer.

10. The method of claim 1, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

11. The method of claim 1, wherein said access policy specifies which applications are allowed Internet access.

12. The method of claim 1, wherein said access policy specifies applications that are allowed Internet access.

13. The method of claim 12, wherein said applications are specified by executable name and version number that are acceptable.

14. The method of claim 12, wherein said applications are specified by digital signatures that are acceptable.

15. The method of claim 14, wherein said digital signatures are computed using a cryptographic hash.

16. The method of claim 15, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

17. The method of claim 1, wherein said access policy specifies Internet access activities that are permitted or restricted for applications or versions thereof.

18. The method of claim 1, wherein said access policy specifies rules that are transmitted to client computers from a remote location.

19. The method of claim 18 wherein said remote location comprises a centralized location for maintaining said access policy.

20. The method of claim 1, wherein said step of blocking Internet access includes:

determining, based on identification of a particular client computer or group thereof, a specific subset of rules filtered for that particular client computer or group thereof.

21. The method of claim 1, wherein said challenge includes a request for a particular client computer to respond as to whether it is in compliance with said access policy.

22. The method of claim 1, further comprising:

redirecting a client computer that is not in compliance with said access policy to a sandbox server; and

informing such client computer that it is not in compliance with said access policy.

23. The method of claim 22 further comprising:

redirecting a client computer that is not in compliance with a particular access policy, to a particular port on the sandbox server; and

displaying particular error message pages on the sandbox server in response to

communications on particular ports.

24. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:

transmitting a plurality of challenges over a period of time from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy during said period of time;

transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued; and

redirecting a request for Internet access by any client computer that does not respond appropriately to any challenge issued to it to a sandbox server.

25. The method of claim 24, further comprising:

displaying an error message on the sandbox server to any client computer that does not respond appropriately to said challenge.

26. The method of claim 25, further comprising:

after display of such error message, permitting said client computer to elect to access the Internet.

27. The method of claim 24, wherein a client computer that responds with a particular predefined code indicating non-compliance is redirected to said sandbox server.

28. The method of claim 24, wherein a client computer that responds with a particular predefined code indicating compliance is permitted Internet access.

29. The method of claim 24, further comprising:

before receipt of a challenge, transmitting an initial message from a particular client computer to the client premises equipment, for requesting the client premises

equipment to transmit a challenge to that particular client computer.

30. The method of claim 29, wherein said initial message comprises a "client hello" packet.

31. The method of claim 24, wherein said client premises equipment is capable of permitting Internet access by selected client computers and redirecting other client computers to the sandbox server.

32. The method of claim 24, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

33. The method of claim 24, wherein said access policy specifies which applications are allowed Internet access.

34. The method of claim 24, wherein said access policy specifies executable names and version number of applications that are allowed Internet access.

35. The method of claim 24, wherein said access policy specifies Internet access activities that are permitted or restricted for applications or versions thereof.

36. The method of claim 24, wherein said access policy specifies rules that are transmitted to client computers from a remote location.

37. The method of claim 36, wherein said remote location comprises a centralized location for maintaining said access policy.

38. The method of claim 24, wherein said step of redirecting a request for Internet access by a client computer includes:

determining, based on identification of a particular client computer or group thereof, a specific subset of rules filtered for that particular client computer or group

thereof.

39. The method of claim 24, wherein said challenge includes a request for a particular client computer to respond as to whether it is in compliance with said access policy.

40. The method of claim 24, further comprising:

redirecting a client computer that is not in compliance with a particular access policy, to a particular port on the sandbox server; and

displaying particular error messages on the sandbox server in response to communications on particular ports.

41. The method of claim 24, further comprising:

permitting client computers that are not in compliance with particular access policies to elect to access the Internet; and

blocking computers that are not in compliance with other access policies from accessing the Internet.

42. The method of claim 24, wherein said access policy specifies which applications are allowed Internet access, and wherein said applications are specified by digital signatures which are acceptable.

43. The method of claim 42, wherein said digital signatures are computed using a cryptographic hash.

44. The method of claim 43, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

45. A system for regulating Internet access by client computers comprising:

an access policy governing Internet access by said client computers;

client premises equipment serving a routing function for each client computer to

be regulated and capable of issuing a plurality of challenges over a period of time to each client computer, for determining whether a given client computer is in compliance with said access policy during said period of time;

one or more client computers which can connect to the Internet and at least one of which can respond to challenges issued by said client premises equipment; and

an enforcement module for selectively blocking Internet access to the Internet for any client computers that fail to respond in a manner that would establish that they are in compliance with said access policy.

46. The system of claim 45, wherein said client premises equipment includes a router.

47. The system of claim 45, wherein said access policy is provided at each client computer to be regulated.

48. The system of claim 45, wherein said enforcement module is provided at said client premises equipment.

49. The system of claim 45, wherein said at least one client computer which can respond to challenges responds with a particular predefined code indicating noncompliance with said access policy and is blocked from Internet access.

50. The system of claim 45, wherein a client computer that responds with a particular predefined code indicating compliance with said access policy is permitted Internet access.

51. The system of claim 45, wherein at least one of the client computer is capable of transmitting an initial message to the client premises equipment before receipt of a challenge, for requesting the client premises equipment to transmit a challenge to that particular client computer.

52. The system of claim 45, wherein said enforcement module is capable of permitting Internet access by selected client computers and denying access to other client computers.

53. The system of claim 45, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

54. The system of claim 53, wherein said enforcement module is capable of determining, based on identification of a particular client computer or group thereof, a specific subset of said access policies filtered for that particular client computer or group thereof.

55. The system of claim 45, wherein said access policy specifies applications that are allowed Internet access.

56. The system of claim 55, wherein said applications are specified by executable name and version number that are acceptable.

57. The system of claim 55, wherein said access policy specifies types of activities which applications are allowed to perform or restricted from performing.

58. The system of claim 55, wherein said applications are specified by digital signatures that are acceptable.

59. The system of claim 58, wherein said digital signatures are computed using a cryptographic hash.

60. The system of claim 59, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

61. The system of claim 45, further comprising:

a sandbox server to which client computers that are not in compliance with said access policy are redirected.

62. The system of claim 61, wherein said sandbox server informs non-compliant client computers that they are not in compliance with said access policy.

63. The system of claim 62, wherein said client computers client computers may elect to access the Internet after being informed that they are not in compliance with said access policy.

64. The system of claim 61, wherein:

said enforcement module is capable of redirecting a client computer that is not in compliance with a particular access policy to a particular port on the sandbox server; and

said sandbox server is capable of displaying particular error message pages in response to communications on particular ports.

9. EVIDENCE APPENDIX

This Appeal Brief is not accompanied by an evidence submission under §§ 1.130, 1.131, or 1.132.

10. RELATED PROCEEDINGS APPENDIX

Pursuant to Appellant's statement under Section 2, this Appeal Brief is not accompanied by any copies of decisions.